Effective Date: 6/28/2005
Revised Date: 9/11/2017
Review Date: 9/11/2017

North Sound Behavioral Health Organization

Section 4000 – Information Systems: Privacy and Security Plan

Authorizing Source: North Sound BHO
Cancels: Approved by: Executive Director
See Also:
Responsible Staff: IS Specialist Signature: Date: 10/3/2017

POLICY #4009.00

SUBJECT: PRIVACY AND SECURITY PLAN

BACKGROUND

The use of computers and computer networks has become an integral part of the behavioral health and human services industry. These technologies have brought and will continue to bring enormous advantages to our industry and will continue to enable us to innovate in the means of delivering service to individuals. These technologies have also brought significant risks regarding individual confidentiality and privacy. Many organizations have opted to establish security and privacy policies that give specific guidelines on an employee's use of these technologies, in all locations. The requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 require such policies be established, enforced and audited.

POLICY

It is the policy of North Sound Behavioral Health Organization (North Sound BHO) that all employees must preserve the integrity and the confidentiality of health and other sensitive information pertaining to our individuals. The purpose of this policy is to ensure North Sound BHO employees have the necessary information to carry out its responsibilities while protecting the confidentiality of individual information. To that end, North Sound BHO employees will:

1. Collect and use protected health information (PHI) only for the purposes of supporting the delivery, payment, integrity and quality of mental health services. North Sound BHO employees and agents will not use or supply PHI for non-health care uses, such as, direct marketing, employment, or credit evaluation processes.
2. Collect and use individual health information only:

    a. As a basis for required reporting of health information;
    b. To receive reimbursement for services provided; or
    c. For research and similar purposes designed to improve the quality and reduce the cost of health care.

3. Recognize PHI collected about individuals must be accurate, timely, complete and available when needed. North Sound BHO employees will:

a. Use their best efforts to ensure the accuracy, timeliness and completeness of data to ensure authorized personnel can access it when needed.
b. Maintain records for the retention periods required by law and professional standards.
c. Implement reasonable measures to protect the integrity of all data maintained about individuals.
d. Recognize individuals have a right of privacy. North Sound BHO employees will respect individuals' dignity at all times. North Sound BHO employees will respect individuals' privacy to the extent consistent with providing the highest quality health care possible and with the efficient administration of the facility.

4. Act as responsible information stewards and treat all individual data and related financial, demographic and lifestyle information as sensitive and confidential. Consequently, North Sound BHO employees will:

   a. Treat all individual data as confidential in accordance with professional ethics and legal requirements.
   b. Not divulge PHI unless the individual (or his or her personal representative) has properly authorized the disclosure or the disclosure is otherwise authorized by law.
   c. When releasing PHI, take appropriate steps to prevent unauthorized re-disclosures, such as, specifying the recipient may not further disclose the information without individual's authorization or as allowed by law.
   d. Implement reasonable measures to protect the confidentiality of information maintained about individuals.
   e. Remove individuals' identifiers when appropriate, such as, in statistical reporting and in research studies.
   f. Not disclose financial or other individual information except as necessary for billing or authorized purposes as authorized by law and professional standards.

5. Recognize mental health information is particularly sensitive, as is HIV/AIDS information, developmental disability information, alcohol and drug abuse information and other information about sexually transmitted or communicable diseases and disclosure of such information could severely harm individuals, such as, causing loss of employment opportunities and insurance coverage, as well as, the pain of social stigma. Consequently, North Sound BHO employees will treat such information with additional confidentiality protections as required by law, professional ethics and accreditation requirements.
6. All employees of North Sound BHO must adhere to this policy. North Sound BHO must adhere to this policy. North Sound BHO will not tolerate violations of this policy. Violation of this policy is grounds for disciplinary action, up to and including termination of employment and criminal or professional sanctions in accordance with North Sound BHO clinical information sanction policy, personnel rules and regulations.

a. Reporting Security Problems

i. If sensitive North Sound BHO information is, or is suspected of, being lost or disclosed to unauthorized parties, the Privacy Officer must be notified immediately.

ii. If any unauthorized use of North Sound BHO's information systems has taken place, or is suspected of taking place, the Security Officer and Privacy Officer must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Security Officer and Privacy Officer must be notified immediately.

b. Additional Responsibilities

As defined below, North Sound BHO employees responsible for Internet security have been designated to establish a clear line of authority and responsibility.

i. IT Department will establish an Internet security infrastructure consisting of hardware, software, policies and standards and department staff will provide technical guidance on PC security to all North Sound BHO staff. The IT Department will respond to virus infestations, hacker intrusions and similar events.

ii. IT staff will monitor compliance with Internet security requirements, including hardware, software and data safeguards. Program directors must ensure their staff follows the Internet security policy established in this document. IT staff will also provide administrative support and technical guidance to management on matters related to Internet security.

iii. IS/IT staff will periodically, and no less than annually, conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.

iv. IS/IT staff will check to ensure appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.

v. IS/IT staff will check to ensure user access controls are defined on these systems in a manner consistent with the need-to-know.

vi. North Sound BHO information owners will see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.

vii. North Sound BHO managers will ensure:

1) Employees under their supervision implement security measures as defined in this document.
2) Employees under their supervision delete sensitive (confidential) data from removable media when the data is no longer needed or useful.

3) Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all North Sound BHO documents that address information security.
4) Employees and contract personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.

viii. Users of North Sound BHO Internet connections must:

1) Know and apply the appropriate North Sound BHO policies and practices pertaining to Internet security.
2) Not permit any unauthorized individual to obtain access to North Sound BHO Internet connections.
3) Not use or permit the use of any unauthorized device in connection with North Sound BHO personal computers.
4) Not use North Sound BHO Internet resources (software/hardware or data) for other than authorized company purposes.
5) Maintain exclusive control over and use of his/her password and protect it from inadvertent disclosure to others.
6) Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project and that is not easy to guess (see Access Codes and Password Policy 4002.00).
7) Ensure data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
8) Report to the Security Officer and Compliance Officer any incident that appears to compromise the security of North Sound BHO information resources. These include missing data, virus infestations and unexplained transactions.
9) Access only the data and automated functions for which he/she is authorized during the course of normal business activity.

c. <u>Contact Point</u>

Questions about this policy may be directed to the Security Officer.

d. <u>Disciplinary Process</u>

Violation of these policies may subject employees or contractors to disciplinary procedures up to an including termination.

ATTACHMENTS

None